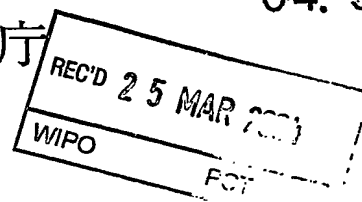


04. 3. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月26日
Date of Application:

出願番号 特願2003-084246
Application Number:
[ST. 10/C]: [JP 2003-084246]

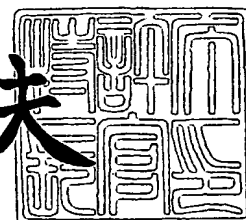
出願人 ソニー株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 1月 5日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0390100902

【提出日】 平成15年 3月26日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/28

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 古城 智雅

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 橋 博紀

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

 【識別番号】 100091546

 【弁理士】

 【氏名又は名称】 佐藤 正美

 【電話番号】 03-5386-1775

【手数料の表示】

 【予納台帳番号】 048851

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9710846

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク接続の管理方法および電子機器

【特許請求の範囲】

【請求項 1】

電子機器が、

LANケーブルの接続の有無を検出するアクセスコントローラと、

マイクロコンピュータと

を有する場合に、

アプリケーションを実行するとき、上記アクセスコントローラの検出出力をチェックすることにより、上記LANケーブルおよび上記電子機器側に、ネットワーク接続に関係する異常があるかどうかの第1のチェックを実行し、

この第1のチェックの結果、上記ネットワーク接続に関係する異常がないときには、上記アプリケーションを実行し、

このアプリケーションが上記ネットワークを使用するとき、上記アクセスコントローラにより上記ネットワークとのリンクが正常であるかどうかの第2のチェックを実行し、

この第2のチェックの結果、上記ネットワークとのリンクが正常なときには、上記アプリケーションの上記ネットワークへのアクセスを実行する

ようにしたネットワーク接続の管理方法。

【請求項 2】

請求項 1 に記載のネットワーク接続の管理方法において、

上記第1のチェックの結果、上記ネットワーク接続に異常があるときには、これを表示し、

上記第2のチェックの結果、上記ネットワークとのリンクが異常のときには、これを表示する

ようにしたネットワーク接続の管理方法。

【請求項 3】

LAN用のコネクタジャックと、

このコネクタジャックに、LANケーブルの接続の有無があったとき、これを

検出するアクセスコントローラと、

このアクセスコントローラの検出出力が供給されるマイクロコンピュータとを有し、

上記マイクロコンピュータは、

アプリケーションを実行するとき、上記アクセスコントローラの検出出力をチェックすることにより、上記LANケーブルおよび上記自機側に、ネットワーク接続に関する異常があるかどうかの第1のチェックを実行し、

この第1のチェックの結果、上記ネットワーク接続に関する異常がないときには、上記アプリケーションを実行し、

このアプリケーションが上記ネットワークを使用するとき、上記アクセスコントローラにより上記ネットワークとのリンクが正常であるかどうかの第2のチェックを実行し、

この第2のチェックの結果、上記ネットワークとのリンクが正常なときには、上記アプリケーションの上記ネットワークへのアクセスを実行するようにした電子機器。

【請求項4】

請求項3に記載の電子機器において、

上記第1のチェックの結果、上記ネットワーク接続に異常があるときには、これを表示し、

上記第2のチェックの結果、上記ネットワークとのリンクが異常のときには、これを表示する

ようにした電子機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ネットワーク機能を有する電子機器において、ネットワークとの接続に異常があったとき、その異常個所を切り分けることのできるようにしたネットワーク接続の管理方法および電子機器に関する。

【0002】

【従来の技術】

パーソナルコンピュータやAV機器などの電子機器が、ネットワークを通じて各種のデータをやりとりする機会が多くなっている。このため、ネットワーク機能を有する電子機器は、ネットワークを通じてデータをやりとりするとき、例えば図4に示すようにしてネットワークの状態をチェックしている。

【0003】

すなわち、図4は、パーソナルコンピュータにおいて実行されるアプリケーションの処理内容をルーチン200として示す。そして、例えばユーザがこのアプリケーションの起動を指示すると、パーソナルコンピュータの処理がルーチン200のステップ201からスタートし、次にステップ202において、ユーザの指示したアプリケーションの本体部分（コア部分）が起動され、続いて、ステップ203において、そのアプリケーションの本体部分の処理が実行される。

【0004】

そして、ステップ203によりアプリケーションの本体部分の処理を実行しているときに、ネットワークを使用する状態になると、処理はステップ204に進み、ネットワークの状態がチェックされる。そして、このチェックの結果、ネットワークが正常なときには、処理はステップ205に進み、ネットワークを使用してデータがアクセスされ、その後、ステップ203に戻ってその処理が続行される。

【0005】

一方、ステップ204のチェックの結果、ネットワークに異常があるときには、処理はステップ206に進み、例えばネットワークに異常のあることがディスプレイに表示され、その後、処理はステップ203に戻る。

【0006】

つまり、ルーチン200においては、ネットワークを使用するときになると、そのネットワークの正常・異常をチェックし、そのチェック結果に対応した処理を実行するようにされている。

【0007】

また、ネットワークに接続された電子機器が実際に動作可能であるかどうかを

確認する方法も開発されている（例えば、特許文献1 参照）。

【0008】

【特許文献1】

特開 2001-358730 公報

【0009】

【発明が解決しようとする課題】

ところで、ネットワークに異常を生じる場合、その理由は以下の2つに大別できる。

(1) 自機におけるトラブル

これは、LANケーブルの抜けや不具合、あるいはLANボードの異常などのように、ユーザが管理できる範囲にトラブルを生じている場合である。

(2) 外部（自機以外）のトラブル

これは、DNSサーバのダウン、トラフィックの混雑などのように、ユーザが管理できない範囲にトラブルを生じている場合である。

【0010】

ところが、OSやアプリケーションから見た場合、(1)項と(2)項とを区別することはできない。また、(2)項のDNSサーバのダウンなどのときには、75～80秒のタイムアウト待ちが発生する。

【0011】

このため、ネットワークの使用中に(1)項のLANケーブルの抜けが起きたときでも、あるいはネットワークの使用前からLANケーブルの抜けが起きていたときでも、ステップ204からステップ206に進むまでに、75～80秒のタイムアウト期間を待つ必要があり、そのタイムアウト期間はユーザの要求に応答しなくなる。そして、ユーザはそのタイムアウト期間後に、ステップ206により何か異常のあることを知ることになる。

【0012】

つまり、自機が原因でネットワークを使用できない状態になったときでも、これをすぐには知ることができない。しかも、自機が原因であるということさえ知ることができない。

【0013】

この発明は、以上のような点にかんがみ、ネットワークの使用に異常があるとき、(1)項と(2)項とを区別することができ、また、(1)項に起因する異常のときには、これをユーザにただちに通知することができるようにするものである。

【0014】

【課題を解決するための手段】

この発明においては、例えば、

電子機器が、

LANケーブルの接続の有無を検出するアクセスコントローラと、

マイクロコンピュータと

を有する場合に、

アプリケーションを実行するとき、上記アクセスコントローラの検出出力をチェックすることにより、上記LANケーブルおよび上記電子機器側に、ネットワーク接続に関する異常があるかどうかの第1のチェックを実行し、

この第1のチェックの結果、上記ネットワーク接続に関する異常がないときには、上記アプリケーションを実行し、

このアプリケーションが上記ネットワークを使用するとき、上記アクセスコントローラにより上記ネットワークとのリンクが正常であるかどうかの第2のチェックを実行し、

この第2のチェックの結果、上記ネットワークとのリンクが正常なときには、上記アプリケーションの上記ネットワークへのアクセスを実行する

ようにしたネットワーク接続の管理方法とするものである。

したがって、LANケーブルや自機でトラブルを生じたときと、ネットワーク側でトラブルを生じたときとで、処理が切り分けられる。

【0015】

【発明の実施の形態】

図1はこの発明の一例を示し、この例においては、OSとしてLinux（登録商標）を搭載したAV機器10を、イーサネット（登録商標）のコネクタプラグ2

1 および LAN ケーブル 22 を通じて ネットワーク 23 に接続する場合である。

【0016】

そして、AV 機器 10 は、この発明に係るハードウェアとして、イーサネット（登録商標）用のコネクタジャック 11 と、アクセスコントローラ 12 と、システム制御用のマイクロコンピュータ 13 とを有する。この場合、コネクタジャック 11 には、コネクタプラグ 21 が差し込まれ、この AV 機器 10 が LAN ケーブル 22 を通じて ネットワーク 23 に接続される。

【0017】

また、アクセスコントローラ 12 は、コネクタジャック 11 とマイクロコンピュータ 13 との間に接続され、後述するネットワークデバイスドライバの制御にしたがって、ネットワーク 23 とのリンク処理やデータのアクセスに必要な処理を実行する。さらに、アクセスコントローラ 12 は、ネットワーク 23 との電気的な接続状態を検出し、その接続状態が変化したとき、これをハードウェア割り込みによりマイクロコンピュータ 13 に通知する機能を有する。

【0018】

すなわち、コネクタプラグ 21 がコネクタジャック 11 に正しく差し込まれると、コネクタジャック 11 の所定の接点の電位が変化し、これがアクセスコントローラ 12 により検出される。そして、アクセスコントローラ 12 は、その電位変化を検出すると、マイクロコンピュータ 13 にハードウェア割り込みをかけ、マイクロコンピュータ 13 に LAN ケーブル 22 の接続されたことを通知する。しかし、コネクタプラグ 21 が差し込まれていないときには、アクセスコントローラ 12 による割り込みはかからない。

【0019】

また、コネクタプラグ 21 がコネクタジャック 11 に正しく差し込まれている状態から抜かれると、やはりコネクタジャック 11 の所定の接点の電位が変化するので、これをアクセスコントローラ 12 が検出してマイクロコンピュータ 13 にハードウェア割り込みをかけ、コネクタプラグ 21 が抜かれたことを通知する。したがって、マイクロコンピュータ 13 は、コネクタプラグ 21（LAN ケーブル 22）の着脱をアクセスコントローラ 12 によるハードウェア割り込みによ

り知ることができる。

【0020】

なお、以上のような機能を有するアクセスコントローラ12として、National Semiconductor Corporation (アメリカ) のIC「DP83815」があり、データのアクセスに関係する信号と、接続状態およびハードウェア割り込みに関係する信号とが別個の外部ピンに割り当てられている。

【0021】

また、マイクロコンピュータ13は、これが実行するソフトウェアの一部として、ネットワークデバイスドライバntwrkおよびネットワークライブラリntwrklibを有する。この場合、ネットワークデバイスドライバntwrkは、アクセスコントローラ12を制御することにより、ネットワーク23に対するデータのアクセスを可能とするためのものである。さらに、ネットワークドライバntwrkは、アクセスコントローラ12からの割り込み信号の処理も行う。また、ネットワークライブラリntwrklibは、ネットワークを使用するための各種の基本的なプログラムの集まりである。

【0022】

さらに、マイクロコンピュータ13には、このAV機器10を使用するときに必要なあるいは有用な複数のアプリケーションA～Nが用意されるとともに、これらアプリケーションA～Nは例えば図2に示す構成のルーチン100（ルーチン100A～100N）とされる。

【0023】

このような構成において、例えばユーザが任意のアプリケーションMの起動を指示すると、パーソナルコンピュータの処理が、その指示されたアプリケーションMを構成するルーチン100（ルーチン100M）のステップ101からスタートし、次にステップ102において、アクセスコントローラ12からの割り込みをチェックすることにより、(1)項についてチェックされる。

【0024】

すなわち、上述のように、コネクタプラグ21とコネクタジャック11との接続状態がアクセスコントローラ12により検出され、その検出結果にしたがって

マイクロコンピュータ 13 に対するハードウェア割り込みが制御されるので、このハードウェア割り込みをステップ 102 においてチェックすることにより、(1) 項を原因とするトラブルを生じているかどうかチェックされる。

【0025】

そして、チェックの結果、(1) 項を原因とするトラブルを生じていないときには、処理はステップ 102 からステップ 103 に進み、このステップ 103 において、ユーザの指示したアプリケーションの本体部分が起動され、続いて、ステップ 104 において、そのアプリケーションの本体部分の処理が実行される。

【0026】

そして、ステップ 104 によりアプリケーションの本体部分の処理を実行しているときに、ネットワーク 23 を使用する状態になると、処理はステップ 105 に進み、ネットワーク 23 とのリンク状態がチェックされる。このネットワーク 23 とのリンク状態のチェックは上記(2)項に対応するものであり、ネットワークデバイスドライバ `ntwrk` がアクセスコントローラ 12 を制御することにより実現される。また、このチェックのタイムアウト期間は、上述のように 75～80 秒である。

【0027】

そして、このチェックの結果、ネットワーク 23 とのリンク状態が正常なときには、処理はステップ 105 からステップ 106 に進み、このステップ 106 において、ネットワーク 23 に対して、アクセスコントローラ 12 および LAN ケーブル 22 を通じてデータがアクセスされ、その後、処理はステップ 104 に戻ってアプリケーションの本体部分の処理が続行される。

【0028】

また、ステップ 105 のチェックの結果、ネットワーク 23 とのリンク状態に異常があるときには、処理はステップ 105 からステップ 107 に進み、このステップ 107 において、例えば「ネットワークに異常があり、ネットワークを使用できません。」の文字列がディスプレイ（図示せず）に表示されるとともに、リンクのできないときの処理が実行され、その後、処理はステップ 104 に戻る。

【0029】

一方、ステップ102において、チェックの結果、(1)項を原因とするトラブルを生じているときには、処理はステップ102からステップ111に進み、このステップ111において、例えば「LANケーブルまたは機器に異常があり、ネットワークを使用できません。」の文字列がディスプレイ（図示せず）に表示されるとともに、リンクができないときの処理が実行され、その後、処理はステップ112に進んでルーチン100を終了する。

【0030】

こうして、上述のAV機器10においては、(1)項や(2)項によるトラブルを知ることができるが、この場合、ルーチン100においては、ステップ102により(1)項についてチェックし、ステップ105によりネットワーク23とのリンク状態をチェックするようにしているので、(1)項に起因するトラブルと、(2)項に起因するトラブルとを切り分けることができ、トラブルを生じたときの対処が容易になる。例えば、LANケーブル22（コネクタプラグ21）の抜けているとき、あるいはLANケーブル22を、ストレートケーブルとクロスケーブルとで間違えているとき、容易に知ることができる。

【0031】

また、ルーチン100は、これを実行すると、まず、ステップ102により(1)項についてチェックするので、(1)項に起因するトラブルのときには、75～80秒のタイムアウト期間を待つことがなく、直ちにそのトラブルを知ることができる。

【0032】

さらに、アクセスコントローラ12はもともとネットワーク23との接続に必要なものであるから、ハードウェアを追加する必要がなく、したがって、コストの上昇を抑えることができる。また、アプリケーションA～Nのどれも、ルーチン100の構成とすることができ、ネットワークを使用するときのトラブル対策をルール化することができる。しかも、以上の処理をLinux（登録商標）のもとで実現することができる。

【0033】

なお、上述においては、1度起動すると、ネットワーク23へのアクセスが、複数回あり得るアプリケーションの場合であるが、例えば電子メールを送受信するソフトウェアのように、1度の起動で1度しかネットワーク23にアクセスしないアプリケーションの場合には、そのルーチン100を図3に示すように構成することができる。

【0034】

すなわち、例えばパーソナルコンピュータにメーラの自動実行を設定した場合には、そのメーラは例えば10分に1度実行されるとともに、1回の実行ごとに1回だけネットワーク23にアクセスする。したがって、このようなアプリケーションの場合には、図3に示すように、ステップ106、107を実行したら、ステップ108によりルーチン100を終了すればよい。

【0035】

また、上述においては、ステップ111において、トラブルを表示するとしたが、そのような表示が好ましくない場合には、例えば、ステップ111において、エラーフラグを立ててからステップ103に進み、その後、必要なときにそのエラーフラグに対応した処理を実行することもできる。

【0036】

[この明細書で使用している略語の一覧]

AV : Audio and Visual
DNS : Domain Name system
IC : Integrated Circuit
LAN : Local Area Network
OS : Operating System

【0037】

【発明の効果】

この発明によれば、電子機器がネットワークを使用するとき、自機に起因するトラブルと、ネットワークに起因するトラブルとを切り分けることができ、トラブルを生じたときの対処が容易になる。また、自機に起因するトラブルのときには、75～80秒のタイムアウト期間を待たずに、直ちにそのトラブルを知ることが

できる。さらに、ハードウェアを追加する必要がなく、コストの上昇を抑えることができる。

【図面の簡単な説明】

【図 1】

この発明の一形態を示すシステム図である。

【図 2】

この発明の一形態を示すフローチャートである。

【図 3】

この発明の他の形態を示すフローチャートである。

【図 4】

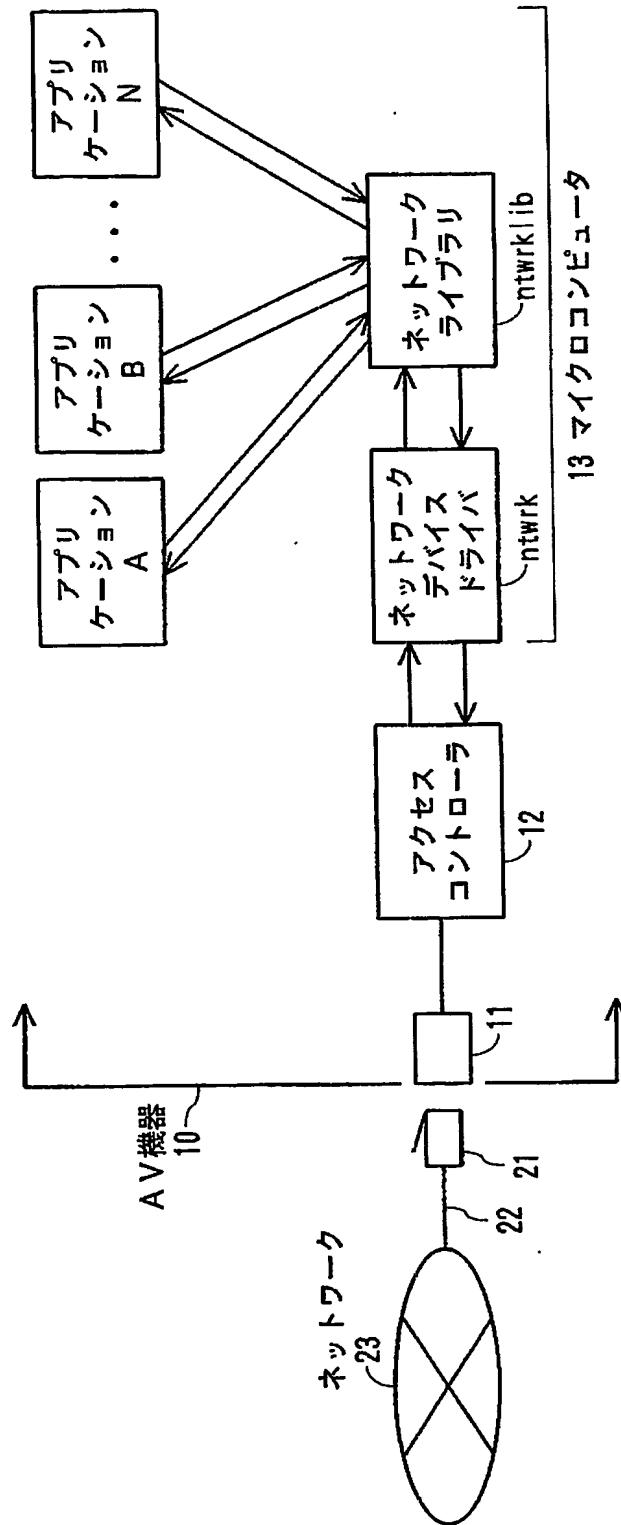
この発明を説明するためのフローチャートである。

【符号の説明】

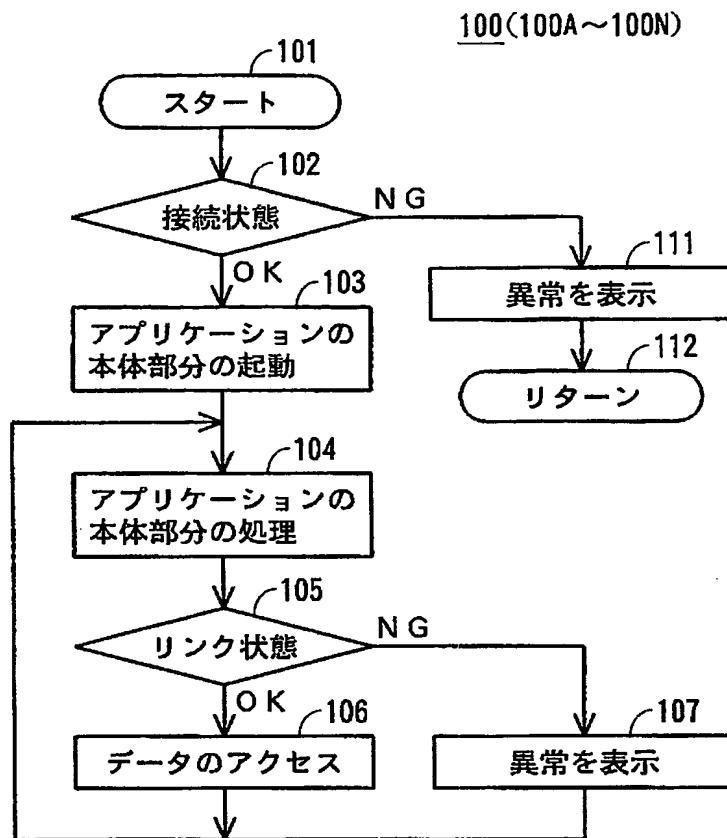
10…AV機器、11…コネクタジャック、12…アクセスコントローラ、13…マイクロコンピュータ、21…コネクタプラグ、22…LANケーブル、23…ネットワーク、ntwrk…ネットワークデバイスドライバ、ntwrklib…ネットワークライブラリ

【書類名】 図面

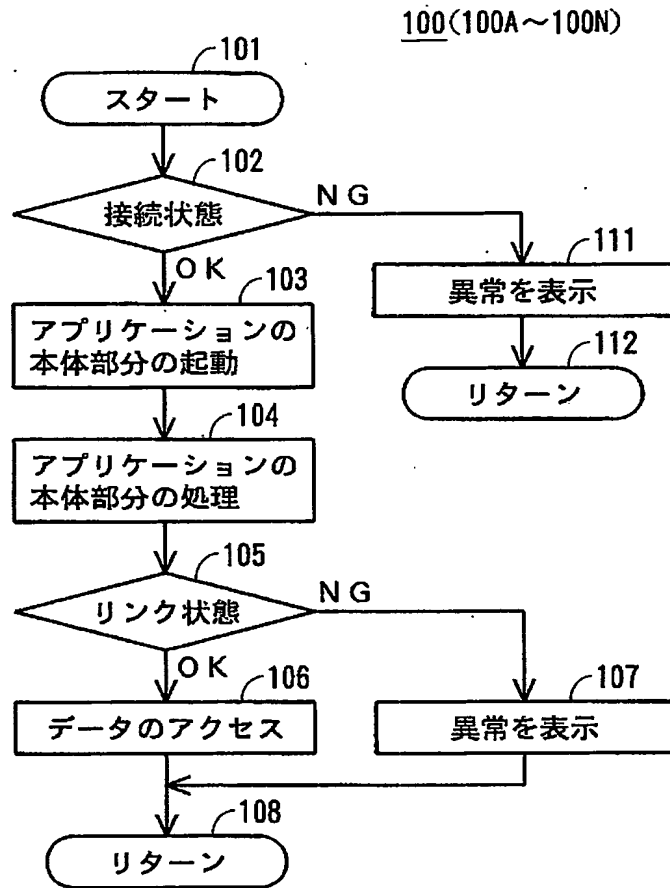
【図 1】



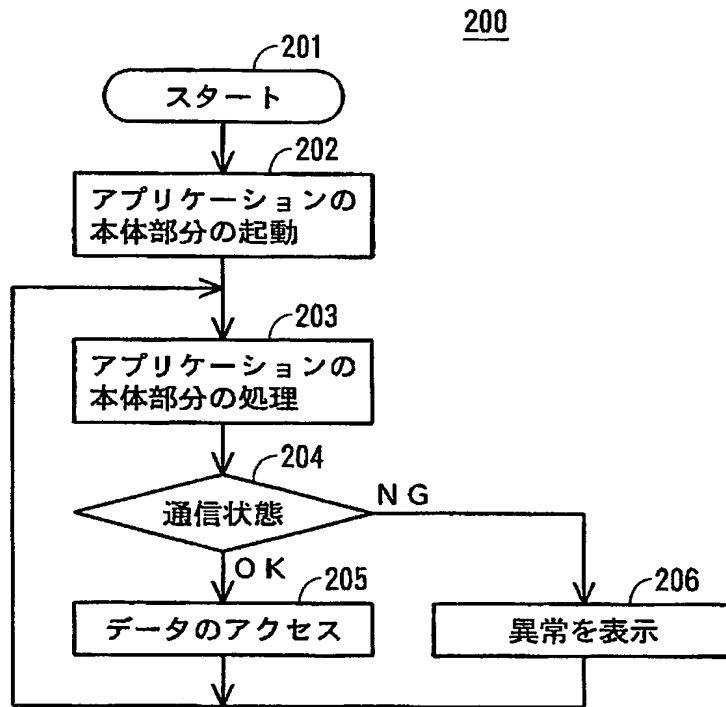
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 ネットワーク接続の異常が自機側とネットワーク側とのどちらが原因であるかを切り分けて検出する。

【解決手段】 LANケーブル22の接続の有無を検出するアクセスコントローラ12を設ける。マイクロコンピュータ13は、アプリケーションを実行するとき、アクセスコントローラ12の検出出力をチェックすることにより、LANケーブル22および自機側に、ネットワーク接続に関係する異常があるかどうかをチェックする。このチェックの結果、異常がないときには、アプリケーションを実行する。このアプリケーションがネットワークを使用するとき、アクセスコントローラ12によりネットワークとのリンクが正常であるかどうかをチェックする。このチェックの結果、正常なときには、アプリケーションのネットワークへのアクセスを実行する。

【選択図】 図1

特願 2003-084246

出願人履歴情報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社